REMARKS

Claims 1-3, 5, 7-13, 18-24, and 28-31 are currently pending in this application. Claims 1-3, 5, 7-13, 18-24 and 28-31 have been rejected. Claims 4, 6 and 25 have been previously cancelled. Claims 14-17 and 26-27 have been previously withdrawn. The response amends claims 1, 2, 18, 23, 28, and 29, leaving for Examiner's consideration claims 1-3, 5, 7-13, 18-24, and 28-31. Reconsideration and withdrawal of the rejection set forth in the Office Action dated November 15, 2007, are respectfully requested.

Claim Objections

Claim 1 is objected to because of the following informalities: the phrase "substantially" in lines 19 renders the claim indefinite because it is unclear what is intended metes and bound of the claim.

The phrase "substantially" has been removed from claim 1 and the Applicant respectfully requests that this objection be withdrawn.

Claim Rejections Based on Prior Art

Claims 1-3, 5, 8-13, 18-24 and 28-31 are rejected under 35 USC §103(a) as being unpatentable over *Lewis, et al.* (US Patent No. 6,233,565 B1) herein referred to as Lewis in view of *Bellwood, et al.* (US Patent No. 6,584,567 B1) herein referred to as Bellwood.

The Cited Prior Art

Lewis

Lewis apparently discloses:

> A system and methods for conducting Internet based financial transactions between a client and a server... A transaction module is included wherein, in response to the client and server being authenticated, the client issues a transaction request to the server and the transaction

> server, in response to a client transaction request, executes an electronic payment transaction at the server and records the transaction in the transaction database... In addition, a third party seller having a processor and a database can be connected via a communication channel to the server, wherein the client further obtains a registration certificate representative of being a consumer registered with said third party seller. A third party credit facility also may be connected via a communication link to the server, for implementing credit card transactions. The transaction execution system may be to purchase an amount of postage, to purchase a ticket for air travel or to an entertainment complex or the like. (Abstract).

Lewis does not disclose a first element – "an appliance inserted between the client and the server having a server environment." In Lewis, the transaction server 180 is one of the components of the server environment (RSP server 4 in FIG. 2) and it "will exist on a protected segment behind a firewall 160" (col. 7, lines 19-21) separated from the client 2n by the Internet 30. Consequently, the transaction server 180 is part of the sever 4, not an appliance between the client 2n and the server 4.

As Examiner stated on Page 5 of the Office Action of 11/5/2007, Lewis does not disclose:

a second element that the appliance "evaluates the at least one electronic transaction query for sensitive data", and

a third element "wherein the server is incapable of distinguishing between data from the client that does not pass through the appliance and data from the client that was intercepted by the appliance."

In addition, Lewis does not disclose a fourth element that the appliance "encrypts the specified sensitive data." In Lewis, "all purchase and refund requests will be digitally signed and encrypted for transmission from the hosts 10n to the transaction server 180" (col. 14, lines 26-28). Thus, it's the host 10n where client 2n resides (FIG.

2), not the transaction server 180 (purported to be between the client 2n and the server 4), which encrypts the data.

Lewis also does not disclose a fifth element that the appliance "decrypts the encrypted sensitive data in response to the at least one electronic information query." In Lewis, such decryption is performed by security server 315 residing on master server 300 (FIG. 3), not the transaction server 180 purported to be between the client 2n and the server 4, wherein the transaction server "receives the purchase request" and "interacts" with the security server 315 "to verify the user's digital signature and to decrypt the transmitted file" (col. 16, lines 63-67). Thus, there is no appliance between the client and the server that decrypts the encrypted sensitive data in response to the at least one electronic information query.

Bellwood

Bellwood apparently discloses:

> A method of enabling a proxy to participate in a secure communication between a client and a set of servers. The method begins by establishing a first secure session between the client and the proxy. Upon verifying the first secure session, the method continues by establishing a second secure session between the client and the proxy. In the second secure session, the client requests the proxy to act as a conduit to a first server. Thereafter, the client and the first server negotiate a first session master secret. Using the first secure session, this first session master secret is then provided by the client to the proxy to enable the proxy to participate in secure communications between the client and the first server. After receiving the first session master secret, the proxy generates cryptographic information that enables it to provide a given service on the client's behalf and without the first server's knowledge or participation. (Abstract)

Bellwood does not disclose a first element that the appliance "evaluates the at least one electronic transaction query to specify sensitive data" and a second element that the appliance "encrypts the specified sensitive data." In Bellwood, a proxy is to "participate in a secure session between a client and one or more original servers" (col. 2, lines 20-22). Once "the client sends a secure HTTP request for a service on the original server…, the proxy may decrypt the request, and modify it as needed, and then encrypt the new request and send it to the original server" (col. 6, lines 9-13). The proxy does not evaluate the request to specify sensitive data because the entire request is presumed to be encrypted before being transmitted to the proxy. In addition, the proxy encrypts the entire request without discretion before sending it to the original server, and there is no teaching of selective encryption of only a (sensitive data) part of the request.

As described above, neither Lewis nor Bellwood teaches an appliance "inserted between the client and the server", wherein the appliance "evaluates at least one electronic transaction query to specify sensitive data" and "encrypts the specified sensitive data only." As the applicant repeatedly stressed in arguments presented in the paper responsive to the Office Action dated January 9, 2007 and June 10, 2007, protecting client's sensitive data in the content from being exposed to unauthorized access after the content is sent by the client but before the content reaches the server is of critical importance. The client may not be aware of what should be encrypted, may not be able to encrypt in a manner that is usable by the system, may not be the best place for making encryption decisions, or may not be the best choice for other reasons; while the server may not be completely secure or may have no business knowing certain data.

The Prior Art Distinguished

To render a claim obvious, the prior art, whether considered alone or in combination, must teach each and every element of the claim.

Claim 1

Independent claim 1 includes the language that the appliance "inserted between the client and the server", which

evaluates the at least one electronic transaction query ~~for~~ to specify sensitive data;

encrypts the specified sensitive data only;

As discussed above, both Lewis and Bellwood fail to disclose an appliance "inserted between the client and the server", wherein the appliance "evaluates at least one electronic transaction query to specify sensitive data" and "encrypts the specified sensitive data only" as recited in claim 1. Accordingly, claim 1 is neither anticipated nor rendered obvious by the cited prior art, whether considered alone or in combination.

Claim 2

Independent claim 2 includes the language:

evaluating at least one electronic request received from a client over at least one secure channel established for sensitive data, using a communication protocol, between the client and a server having an associated server environment;

applying at least one cryptographic operation to the sensitive data specified in response to the at least one electronic request, yielding sensitive data in a first form;

Although claim 2 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. Accordingly, claim 2 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason. Claims 3, 5, 7-13, which depend from claim 2, are allowable at least for depending from an allowable base claim and potentially for other reasons, as well.

Claim 18

Independent claim 18 includes the language:

at least one processing device coupled among the at least one server site, the at least one client computer and the at least one network, wherein, in operation, the at least one processing device evaluates at least one electronic request from the at least one client computer to the at least one server site received via the at least one network for sensitive data and applies at least one cryptographic operation specifically to the sensitive data in response to the at least one electronic request;

Although claim 18 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. Accordingly, claim 18 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason. Claims 19-22, which depend from claim 18, are allowable at least for depending from an allowable base claim, and potentially for other reasons as well.

Claim 23

Independent claim 23 includes the language:

at least one processing device coupled among at least one server system and at least one network coupling to evaluate at least one received electronic request in a first protocol format, wherein the at least one processing device:

determines whether the at least one received electronic request includes sensitive data;

encrypts the sensitive data in the at least one received electronic request;

Although claim 23 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. Accordingly, claim 23 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason. Claim 24, which depends from claim 23, is allowable at least for depending from an allowable base claim, and potentially for other reasons as well.

Claim 28

Independent claim 28 includes the language:

means for evaluating the at least one electronic transaction query ~~for~~ to specify sensitive data;

means for encrypting the specified sensitive data only;

Although claim 28 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. Accordingly, claim 28 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason.

Claim 29

Independent claim 29 includes the language:

the pattern specification engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches the server;

the cryptographic engine applies a cryptographic transformation specifically to the sensitive data;

Although claim 29 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. Accordingly, claim 29 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason. Claims 30-31, which depend from claim 29 are allowable at least for depending from an allowable base claim.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-2207, under Order No. 36321-8009.US01 from which the undersigned is authorized to draw.

Dated: February 7, 2008

Respectfully submitted,

By / William F. Ahmann /
William F, Ahmann
Registration No.: 52,548

Customer No. 22918
PERKINS COIE LLP
101 Jefferson Drive
Menlo Park, California 94025-1114
(650) 838-4300
(650) 838-4350 (Fax)
Agent for Applicant